TELECO CHIPS

_ TELECOM ESCUELA TÉCNICA VLC SUPERIOR DE UPV INGENIEROS DE TELECOMUNICACIÓN

SEGURIDAD EN REDES

Introducción a la inseguridad en las redes inalámbricas

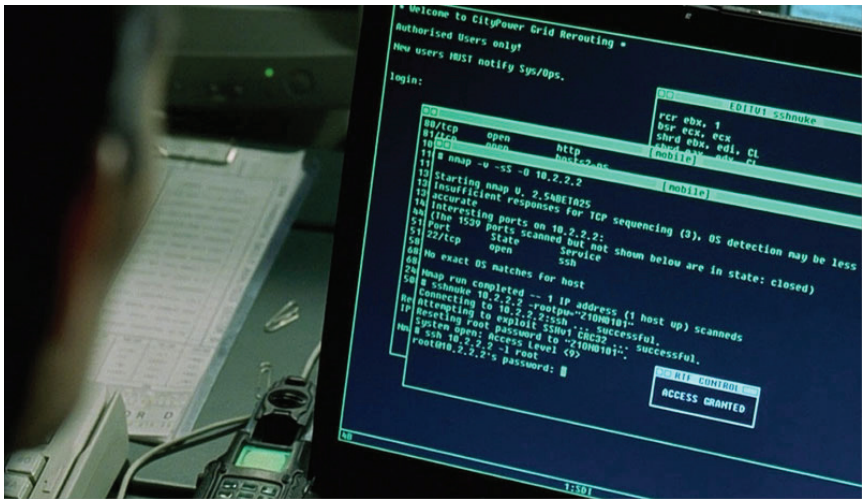
Este telecochip aborda de manera amena las vulnerabilidades de las redes inalámbricas en materia de seguridad.

DESARROLLO

Durante el taller se trata la forma de proteger las redes domésticas y corporativas así como la forma en la que un eventual atacante podría acceder a ellas.

También conoceremos la seguridad en controles de acceso y redes inalámbricas más habituales. Del mismo modo se estudiarán las actuaciones que, una vez dentro, se podrían llevar a cabo y contramedidas efectivas ante un posible ataque.

Todo el proceso se ejemplifica con diversos casos reales y ejemplos en directo con simulaciones de escenarios típicos.



ACTIVIDAD

Durante el taller, los asistentes tienen la oportunidad de comprobar la efectividad de varios protocolos de seguridad, junto a casos reales en los despliegues de varios ISP.

...Y AHORA TÚ

1. Haz una comprobación simple de la seguridad de tu red doméstica, en caso de que sea inalámbrica. ¿**Sabes acceder a tu router?**¿Cuál es tu IP? ¿Y tu usuario y contraseña?
Para acceder al router necesitas averiguar tu dirección (IP) y la contraseña. Normalmente, estos datos vienen apuntados en el propio router, o en el manual de usuario del router o son entregados por tu proveedor de Internet.
Si no es el caso puedes contactar con tu proveedor para que te los facilite.

2. ¿Sabes **qué tipo de protección está configurada** en tu router? ¿Ninguna? ¿WEP? ¿WPA/WPA2?
En el apartado de "Seguridad" de la pestaña "Wireless" debe aparecer el tipo de cifrado utilizado. Como cada marca y modelo tiene su propia interfaz de usuario, se recomienda que se lea el manual de usuario para localizar las opciones con más facilidad. Recordamos que WPA2 es el cifrado más seguro.

3. **¿Se ha cambiado la contraseña** por defecto? ¿Sí? ¿No? Se recomienda encarecidamente cambiar las contraseñas por defecto ya que son contraseñas genéricas que se encuentran disponibles en Internet o se conoce el algoritmo para calcularlas.

4. **¿La contraseña utilizada es lo suficientemente compleja**? ¿Tiene letras y números? ¿Tiene mayúsculas y minúsculas? ¿Tiene una longitud suficiente (aprox. 10 letras)? ¿Tiene símbolos? No es obligatorio que la contraseña tenga todos estos elementos pero cuanta más complejidad agregues más difícil será que un tercero consiga averiguarla.

Amine Taouirsa

es Ingeniero de Telecomunicaciones. Apasionado de la seguridad informática, se dedica a aprender e investigar en ese campo. Pertenece al IEEEsb UPV. Ha impartido varias charlas y talleres, dentro y fuera de la UPV, sobre redes inalámbricas, criptografía, ingeniería inversa y otros temas relacionados con la seguridad.

¿Quieres más? Entra aquí:
museotelecomvlc.etsit.upv.es/telecochips

_ TELECOM ESCUELA TÉCNICA VLC SUPERIOR DE UPV INGENIEROS DE TELECOMUNICACIÓN

UNIVERSITAT POLITÈCNICA DE VALÈNCIA

GOBIERNO DE ESPAÑA · MINISTERIO DE ECONOMÍA Y COMPETITIVIDAD

FECYT FUNDACIÓN ESPAÑOLA PARA LA CIENCIA Y LA TECNOLOGÍA